REMARKS

Applicant respectfully traverses and requests reconsideration.

Applicant wishes to thank the Examiner for the notice that claims 40-44 have been allowed.

As to claim 38, Applicant again respectfully submits that this claim is in condition for allowance as the office action adds limitations into the claim that are not present. For example, with respect to claim 38, the office action alleges that Chan discloses "determination of a digital signature verification error" whereas claim 38 does not include this language. Accordingly this claim is in condition for allowance.

Claims 1-6, 9-14, 17-25, 28-34 and 37 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Chan in view of Schmeidler et al and Bisbee et al. As a preliminary matter, independent claim 17, has not been rejected as claim language in this claim has not been addressed in the office action. For example, claim 17 requires, among other things, "updating a digital signature verification map to add an acceptable message header identifier associated with a public key certificate identifier". Updating such a verification map to add an acceptable message header language has not been addressed in the office action nor can Applicant find such an operation in the cited references. Accordingly, this claim is also believed to be in condition for allowance. Applicants noted this in their last response.

As to other claims, the office action asserts a new ground of rejection, but appears to cite the exact same sections of the Chan reference for allegedly teaching, determining a digital signature verification error based on a received message header identifier associated with a public key certificate identifier and generating a digital signature verification map containing a plurality of acceptable message header identifiers. However, Applicant respectfully submits that

Chan does not teach such operations. The office action also admits that neither Chan nor Schmeidler "teach received message header identifier association with public key, digital signature entity and the mapping."(OA page 3). Also, the office action again does not address Applicant's previous position with respect to the Chan reference nor to the showings requested by Applicant in the previous response. If the rejection is maintained, Applicant again respectfully requests a response. None of the limitations appear to be taught in the Chan reference and as such, the claims are in condition for allowance as further noted below.

As to the Bisbee reference, the Bisbee reference is directed to system and methods for electronic transmission, storage, and retrieval of authenticated electronic original documents and in particular, is directed to the problem of validity periods of digital certificates which expire. As such, Bisbee describes a type of trusted custodian that validates submitted, signed information by testing the integrity of the contents of each signed information object and the validity of the signature of the respective transfer agent and applyies a date and time stamp. One method described includes revalidating an electronic original object by verifying the digital signature of the trusted custodial utility applied to the object and applying to the revalidated object a current date time stamp. The teachings of Bisbee do not appear to be related to the claimed subject matter. In addition, the motivation given in the Office Action for combining the disparate teachings of Chan and Schmeidler with that of Bisbee is that one would do so "in order to revalidate the original object a current time stamp and digital signature in current authentications certificate."(see Office Action). However, the claims are not directed to any such operation and instead the claims are directed to an apparatus and method for providing information security where a received message header identifier is used to determine that a digital sender verification error has occurred and also generating a digital signature verification map that contains a

plurality of acceptable message header identifiers for the public key certificate identifier. Accordingly, the motivation is not relevant to Applicants' claimed invention, and for this reason alone, the claims are in condition for allowance.

Moreover, Bisbee is allegedly cited as disclosing what Schmeidler and Chan lack, namely, generating a digital signature verification map containing a plurality of acceptable message header identifiers associated with the public key certificate identifier, in response to determining a digital signature verification error. However, the cited portions of Bisbee, namely, FIG. 1(a), 23(a), 4(a) and 5(a) and associated text does not describe any such digital signature verification map that contains a plurality of acceptable message header identifiers associated with a public key certificate identifier. This is because Bisbee is directed to a completely different problem and describes a completely different methods and apparatus than that that set forth in Applicants' claims. In fact, as the Bisbee reference states, FIGS. 4(a) and 5(a) actually illustrate an object inventory that is created for a respective deal that is carried out by a transaction unit. As stated in Bisbee, an object inventory is a "list of object identifiers and associated signature blocks for e original corresponding to a deal". As such, this is merely a compilation of digitally signed objects for example that are used in an electronic transaction. In contrast, Applicant claims generating a digital signature verification map containing a plurality of acceptable message header identifiers. The object inventory list has nothing to do with digital signature verification nor is it a digital sender verification map that contains a plurality of acceptable message header identifiers. Accordingly, Applicants respectfully submit that the claims are in condition for allowance.

In addition, Chan is directed to a system that can protect against unruly executable content that is downloaded, for example, from the Internet (see for example, page 1, paragraph

5). The Chan reference does not appear to teach or suggest the claimed method or apparatus since among other things, it does not appear to determine a digital signature verification error, such as verifying a digital signature of a certificate based on received message header identifier associated with a public key certificate identifier as required in the claim.

The cited portion of the Chan reference (page 8, 2nd column, 3rd paragraph and page 9, 1st column, 1st paragraph and page 10, 1st column, 2nd paragraph) is not directed to a digital signature verification process or to the detection of an error based on a digital signature verification process that is based on received message header identifier associated with a public key certificate identifier. Instead, the cited portion refers to a calling process being checked to see if it is restricted by an appropriate restricted security identifier in a token. As best understood, this process does not appear to be performed by a digital signing verification process that is based on a received message header ID that is associated with a public key certificate identifier as required by the claim. In fact, it does not appear that the described token is digitally signed nor does it appear that a message header identifier that is associated with a public key certificate identifier is used in any digital signature verification process. As such, the claims are in condition for allowance.

In addition, the reference also appears to fail to teach generating a digital signature verification map as claimed. The office action cites to page 8, 1st column, 3rd paragraph and page 9, 2nd column, 3rd and 4th paragraphs. However, as best understood, paragraph 82 of the cited reference describes for example, that a URL string is converted to a restricted security ID through a one-way cryptographic hash function to convert the URL stream to a restricted security identifier by adding a header indicating that the number is a security ID identifier and how the number was generated. This portion describes generating a security identifier. There is no

digital signature verification map that includes a plurality of acceptable message header identifiers that is associated with a public key certificate identifier. In fact, it does not appear that any digital signature verification operation is described in the cited portions, nor is there a reference to a plurality of acceptable message header identifiers that are contained in a digital signature map as required by the claim. Accordingly, the claims are in condition for allowance based on this reason also.

The Schmeidler reference has allegedly been cited for teaching what Chan lacks. However, Schmeidler only appears to be cited as teaching that a digital signature is associated with a corresponding public key. However, Applicant respectfully submits that the Patent Office appears to be selectively dissecting the claim in a manner that fails to address the claim language properly. In any event, Chan fails to teach the subject matter for which is has been cited and therefore the claims are allowable.

Moreover, the motivation given in the office action to combine Chan and Schmeidler appears to be irrelevant to the claimed invention as the motivation for combining the teachings of Chan and Schmeidler is that one would combine the references to protect the value of the content and prevent unauthorized use and copying of the content. However, the claims are directed instead to an apparatus and method for providing information security where a received message header identifier is used to determine if a digital signature verification error has occurred and also generating a digital signature verification map that contains a plurality of acceptable message header identifiers for the public key certificate identifier. As described in Applicant's specification, Applicant's apparatus and method can overcome a problem in which an attacker may change a transport header indicating that a message is coming from a different source, not to

preventing unauthorized copying of content as described in the Schmeidler reference. Accordingly, claims 1 and 10 are in condition for allowance.

As to claim 20, Applicant respectfully reasserts the relevant remarks made above with respect to claim 1 and as such this claim is also in condition for allowance.

As to claim 29, Applicant respectfully reasserts the relevant remarks made above with respect to claim 1 and as such this claim is also in condition for allowance.

Claim 38 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Chan in view of Schmeidler and Bisbee as applied to claims 1, 10, 20 and 29 and further in view of Cooper et al. As noted above, Applicant again respectfully submits that this claim is in condition for allowance as the office action adds limitations into the claim that are not present. For example, with respect to claim 38, the office action alleges that Chan discloses "determination of a digital signature verification error" whereas claim 38 does not include this language. Accordingly, Applicant respectfully submits that a prima facia showing of obviousness has not been presented and as such, the claim is in condition for allowance. In addition, the office action admits that Chan does not describe a trusted alias map and alleges that Cooper teaches such a mechanism. However, Cooper is also silent as to generating a trusted alias map containing the plurality of acceptable message identifiers in at least one associated subject alias. Accordingly, this claim is also believed to be in condition for allowance.

The dependent claims add additional novel and non-obvious subject matter and Applicant respectfully reasserts relevant remarks made with respect to the dependent claims made in previous office actions.

Accordingly, Applicant respectfully submits that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited

to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 9/14/05

By: _____
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P. C.
222 N. LaSalle Street
Chicago, IL 60601
PHONE: (312) 609-7599
FAX: (312) 609-5005
E-MAIL: creckamp@vedderprice.com